IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

Microsoft Corporation,

Plaintiff,

v.

Does 1-10 Operating an Azure Abuse Network,

Defendants.

Civil Action No.

FILED UNDER SEAL

DECLARATION OF JASON LYONS IN SUPPORT OF MICROSOFT'S MOTION FOR TEMPORARY RESTRAINING ORDER AND RELATED RELIEF

I, Jason Lyons, declare as follows:

1. I am a Principal Manager of Investigations in the Digital Crimes Unit ("DCU") Cybercrime Enforcement Team at Microsoft Corporation. I make this declaration based upon my personal knowledge, and upon information and belief from my review of documents and evidence collected during Microsoft's investigation, including conversations with my colleagues Rodel Finones and Maurice Mason.

2. I joined Microsoft's DCU in 2013. During my tenure, Microsoft's DCU has worked to disrupt and deter cybercriminals who set out to misuse Microsoft's products and services for malicious purposes. I know from my work at DCU that despite the great lengths Microsoft goes to prevent abuse and enhance the safety its products and services, cybercriminals remain persistent and continuously innovate their tools and techniques to bypass even the most robust security measures.

3. In my role at Microsoft, I assess technological security threats to Microsoft and the impact of such threats on Microsoft's business and customers. Among my responsibilities is

protecting Microsoft's online service assets from network-based attacks. I also participate in the investigation of malware and in court-authorized countermeasures to neutralize and disrupt malware. For example, I have personally investigated and assisted in the court-authorized takedown of several families of malware or botnets while at Microsoft, including the malware families and botnets known as Ramnit, ZeroAccess, Dorkbot, and Necurs.

4. Before joining Microsoft, I held cybersecurity-related positions for Xerox and Affiliated Computer Services ("ACS"), and in those roles I provided in-court testimony in connection with a temporary restraining order application concerning the misappropriation of ACS's intellectual property. Prior to entering the private sector, from 1998 to 2005, I served as a Counterintelligence Special Agent in the United States Army. My duties as a Counterintelligence Special Agent included investigating and combating cyber-attacks against the United States. I obtained certifications in counterintelligence, digital forensics, computer crime investigations, and digital media collection from the United States Department of Defense. A true and correct copy of my curriculum vitae is attached to this declaration as Exhibit 3.

5. Since about August 2024, I have been investigating the structure and function of an online criminal enterprise ("Azure Abuse Enterprise") responsible for using fraud and deception to breach Microsoft's security systems, misusing authentication credentials stolen from paying Microsoft customers, and gaining unauthorized access to and use of Microsoft computers and software for malicious purposes.

6. The Azure Abuse Enterprise consists of primarily of persons who can be grouped into two general categories. The first group of persons is responsible for working together to provide the software, infrastructure, and stolen Microsoft customer credentials that enable members of the Azure Abuse Enterprise to break into Microsoft's Azure platform and use for

malicious purposes generative AI tools developed by OpenAI. The second group of persons consists of end users of the software and infrastructure provided by the Azure Abuse Enterprise. These persons use the Azure Abuse Enterprise's technology and services to break into Microsoft's systems and use generative AI tools to create harmful content that is then distributed to others.

7. Together, the Azure Abuse Enterprise's collective use of stolen customer credentials, customized software tools, and physical infrastructure has allowed Defendants to steal many thousands of dollars' worth of services from Microsoft and its paying customers and to generate thousands of harmful images that have been distributed over the Internet.

Azure Overview

8. Microsoft is a leader in the field of Artificial Intelligence ("AI"). AI refers to software that imitates human behaviors and capabilities. Microsoft's public documentation explains that AI encompasses a wide range of workloads including:

- Machine Learning ("ML")- the way humans "teach" a computer model to make predictions and draw conclusions from data is often the foundation for an AI system.
- Computer vision – Capabilities within AI to interpret the world visually through cameras, video, and images.
- Natural language processing – Capabilities within AI for a computer to interpret written or spoken language and respond in kind.
- Document intelligence – Capabilities within AI that deal with managing, processing, and using high volumes of data found in forms and documents.
- Knowledge mining – Capabilities within AI to extract information from large volumes of often unstructured data to create a searchable knowledge store.
- Generative AI – Capabilities within AI that create original content in a variety of formats including natural language, image, code, and more. Typically, generative AI applications take in natural language input ("prompts") and return appropriate

responses in a variety of formats including natural language, image, code, and audio.[1]

9. Microsoft's Azure cloud platform is an important part of Microsoft's AI leadership. Originally announced in 2008 as Microsoft's new cloud computing operating system, "Windows Azure" was built as an extension of Windows New Technology ("Windows NT") and marked the beginning of Microsoft's Cloud Platform as a Service offering. "Windows Azure" became commercially available in 2010 and after more than a decade of evolution is known today simply as "Azure."[2]

10. Azure consists of a global network of Microsoft computers and datacenters responsible for hosting, running, and managing Microsoft and third-party software products. Figure 1 below is a true and correct screen capture from an Azure webpage depicting the location of some of Azure's physical infrastructure worldwide. In addition to the Microsoft-owned resources depicted in Figure 1, customers use their own computing resources and publi Internet infrastructure to connect to and use Azure services.[3]

Fig. 1: Azure Global Datacenters

[1] https://learn.microsoft.com/en-us/training/modules/get-started-ai-fundamentals/6-understand-generative-ai; A true and correct copy of which is attached to the Index of Evidence("Index") as Exhibit 10
[2] https://techcommunity.microsoft.com/t5/educator-developer-blog/the-history-of-microsoft-azure/ba-p/3574204; A true and correct copy of which is attached to the Index as Exhibit 11
[3] https://datacenters.microsoft.com/globe/explore/; A true and correct copy of which is attached to the Index as Exhibit 12

11. As explained in Microsoft's Cloud Computing Dictionary, Azure cloud services fall into four broad categories: infrastructure as a service, platform as a service, serverless, and software as a service.[4] These are sometimes called the cloud computing "stack" because they build on top of one another. The most basic category of cloud services is infrastructure as a service ("IaaS"), which allows customers to rent IT infrastructure like servers, virtual machines, storage, networks, and operating systems on a pay-as-you-go basis. Platform as a service ("PaaS") refers to cloud computing services that supply an on-demand environment for developing, testing, delivering, and managing software applications. PaaS is designed to make it easier for developers to quickly create web or mobile apps without worrying about setting up or managing the underlying infrastructure of servers, storage, network, and databases needed for development. Software as a service ("SaaS") is a method for delivering software applications over the Internet on demand and typically on a subscription basis.[5]

12. Azure physical infrastructure is supported by proprietary Microsoft software responsible for enabling communications routing, system monitoring, load balancing, security, providing database and user interface functionality. For example, the Azure portal is a web-based, unified console that lets users create and manage their Azure resources. Users can use the Azure portal to build, manage, and monitor everything from simple web apps to complex cloud deployments. In addition to front end software like Azure portal, Microsoft has created a significant amount of back-end software required to provide Azure functionality.[6]

13. As with most of its commercial software, Microsoft takes steps to protect its copyright interests in Azure software and grants customers licenses to use it under certain conditions. Microsoft's software and computer protection efforts include contracts, technological access controls to Azure computers, and various security measures.

---

[4] https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-are-private-public-hybrid-clouds; A true and correct copy of which is attached to the Index as Exhibit 13

[5] https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-azure; A true and correct copy of which is attached to the Index as Exhibit 14

[6] https://learn.microsoft.com/en-us/azure/azure-portal/azure-portal-overview; A true and correct copy of which is attached to the Index as Exhibit 15

14. A person or company that wishes to use Azure services must first create an Azure account and user profile. Azure users must provide accurate location, name, and contact information and must agree to the Microsoft Customer Agreement.[7] Among other things, the Microsoft Customer Agreement states:[8]

> a) Licenses for Products. Products are licensed and not sold. Upon Microsoft's acceptance of each order and subject to Customer's compliance with this Agreement, Microsoft grants Customer a nonexclusive and limited license to use the Products ordered as provided in this Agreement. These licenses are solely for Customer's own use and business purposes and are nontransferable except as expressly permitted under this Agreement or applicable law.
>
> b) Duration of licenses. Online Services and some Software are licensed on a subscription basis for a specified period of time. Subscriptions expire at the end of the applicable subscription period unless renewed. Some Subscriptions renew automatically until canceled. The Subscription term for Online Services that are billed in arrears based on usage is the same as the billing period unless otherwise specified in the Product Terms. Perpetual Software licenses become perpetual upon payment in full.
>
> c) End Users. Customer will control access to, and use of, the Products by End Users and is responsible for any use of the Products that does not comply with this Agreement.

The Microsoft Customer Agreement also includes a "restrictions" section that expressly prohibits several categories of conduct:

> f) Restrictions. Except as expressly permitted in this Agreement or Product documentation, Customer must not (and is not licensed to):
>
> (i) reverse engineer, decompile, or disassemble any Product or Services Deliverable, or attempt to do so (except where applicable law permits despite this limitation);
>
> (ii) install or use non-Microsoft software or technology in any way that would subject Microsoft's intellectual property or technology to any other license terms;

---

[7] https://signup.azure.com/signup?offer=ms-azr-0044p&appId=102&ref=&redirectURL=https:%2F%2Fazure.microsoft.com%2Fget-started%2Fwelcome-to-azure%3Fsrc%3Dacom_free&l=en-us; A true and correct copy of which is attached to the Index as Exhibit 16

[8] https://www.microsoft.com/licensing/docs/customeragreement; A true and correct copy of which is attached to the Index as Exhibit 26

(iii) work around any technical limitations in a Product or Services Deliverable or restrictions in Product documentation;

(iv) separate and run parts of a Product or Services Deliverable on more than one device;

(v) upgrade or downgrade parts of a Product at different times;

(vi) transfer parts of a Product separately; or

(vii) distribute, sublicense, rent, lease, or lend any Products or Services Deliverables, in whole or in part, or use them to offer hosting services to a third party

15. Some Azure services are provided free of charge, but most require payment. Microsoft provides pricing models that let customers pay only for the cloud resources they use. Azure OpenAI's image processing capabilities are purchased via a tokenization system that provides pricing based on the total number of tokens consumed by image inputs. The number of tokens consumed is calculated based on two main factors: the level of image detail (low or high) and the image's dimensions.[9]

16. After agreeing to the Microsoft Customer Agreement, a user wishing to access and use Azure resources and services must authenticate themselves with valid Microsoft-provided credentials. There are several ways a user can authenticate themselves to gain access to Azure services. For example, users can authenticate themselves to Azure using Microsoft Entra ID, which is a cloud-based identity and access management service. Another way of authenticating and gaining access to Azure is through the use of API Keys.

The Azure OpenAI Service

17. The Azure OpenAI Service is Microsoft's cloud solution for deploying, customizing, and hosting generative AI models created by the company OpenAI. The Azure OpenAI Service provides access to many of OpenAI's generative AI models including versions of OpenAI's GPT and DALL-E models. The Azure OpenAI Service brings together OpenAI's models and APIs with the security and scalability of the Azure cloud platform. Microsoft experts in AI research, policy, and engineering collaborate to develop practical tools and

[9] https://learn.microsoft.com/en-us/azure/ai-services/openai/overview; A true and correct copy of which is attached to the Index as Exhibit 17

methodologies that support AI security, privacy, safety, and quality and embed them directly into the Azure AI platform.[10]

18. Azure OpenAI Service is made available to customers under the terms governing their subscription to Microsoft Azure Services, including Product Terms for Microsoft Azure Services and Microsoft's Code of Conduct.[11] Microsoft's contractual and policy terms prohibit, for example, content that describes, features, or promotes sexual exploitation or abuse, whether or not prohibited by law. This includes erotic, pornographic, or otherwise sexually explicit content; sexually suggestive content, depictions of sexual activity, and fetish content. Microsoft also prohibits content that attacks, denigrates, intimidates, degrades, targets, or excludes individuals or groups on the basis of traits such as actual or perceived race, ethnicity, national origin, gender, gender identity, sexual orientation, religious affiliation, age, disability status, caste, or any other characteristic that is associated with systemic prejudice or marginalization. Microsoft prohibits content that targets individual(s) or group(s) with threats, intimidation, insults, degrading or demeaning language or images, promotion of physical harm, or other abusive behavior such as stalking.

19. In addition to the restrictions and guidelines set forth in customer contracts, the Code of Conduct, the Transparency Note,[12] and Microsoft's AI principles,[13] Microsoft has also developed technical measures controlling access to and enhancing the safety of the Azure OpenAI Service. Microsoft technical measures for protecting the safety of the Azure OpenAI Service include Microsoft's content filtering and abuse detection technologies. Within the Azure OpenAI Service, the OpenAI models are integrated with Microsoft-developed content filtering and abuse detection models.[14] For example, Azure OpenAI Service includes a content filtering

---

[10] https://azure.microsoft.com/en-us/solutions/ai/responsible-ai-with-azure/#features; A true and correct copy of which is attached to the Index as Exhibit 18

[11] https://learn.microsoft.com/en-us/legal/cognitive-services/openai/code-of-conduct?context=%2Fazure%2Fai-services%2Fopenai%2Fcontext%2Fcontext; A true and correct copy of which is attached to the Index as Exhibit 19

[12] https://learn.microsoft.com/en-us/legal/cognitive-services/openai/transparency-note?tabs=text; A true and correct copy of which is attached to the Index as Exhibit 20

[13] https://learn.microsoft.com/en-us/azure/machine-learning/concept-responsible-ai?view=azureml-api-2; A true and correct copy of which is attached to the Index as Exhibit 21

[14] https://learn.microsoft.com/en-us/azure/ai-services/openai/concepts/content-filter?tabs=warning%2Cuser-prompt%2Cpython-new; A true and correct copy of which is attached to the Index as Exhibit 22

system that works alongside core models, including DALL·E image generation models. This system works by running both the prompt and completion through an ensemble of classification models designed to detect and prevent the output of harmful content. The content filtering system detects and takes action on specific categories of potentially harmful content in both input prompts and output completions. The text content filtering models for the hate, sexual, violence, and self-harm categories have been specifically trained and tested on the following languages: English, German, Japanese, Spanish, French, Italian, Portuguese, and Chinese. However, the service can work in many other languages.

20. The content filtering system integrated in the Azure OpenAI Service contains Neural multi-class classification models aimed at detecting and filtering harmful content; the models cover four categories (hate, sexual, violence, and self-harm) across four severity levels (safe, low, medium, and high). Other optional classification models are aimed at detecting jailbreak risk and known content for text and code; these models are binary classifiers that flag whether user or model behavior qualifies as a jailbreak attack or match to known text or source code.

21. Azure OpenAI Service includes default safety applied to all models, with one exception not relevant here. These configurations provide customers with a responsible experience by default, including content filtering models, blocklists, prompt transformation, content credentials, and others.[15] For example, Azure OpenAI DALL·E also comes with prompt transformation by default. This transformation occurs on all prompts to enhance the safety of an original prompt, specifically in the risk categories of diversity, deceptive generation of political candidates, depictions of public figures, protected material, and others.

22. In the default streaming scenario, completion content is buffered, the content filtering system runs on the buffered content, and – depending on the content filtering configuration – content is either returned to the user if it doesn't violate the content filtering

[15] https://learn.microsoft.com/en-us/azure/ai-services/openai/concepts/default-safety-policies; A true and correct copy of which is attached to the Index as Exhibit 23

policy (Microsoft's default or a custom user configuration), or it's immediately blocked and returns a content filtering error, without returning the harmful completion content. This process is repeated until the end of the stream. Content is fully vetted according to the content filtering policy before it's returned to the user.[16]

23. In addition to the content filtering system, Azure OpenAI Service performs Abuse Monitoring to detect content and/or behaviors that suggest use of the service in a manner that might violate applicable product terms. Azure OpenAI Service detects and mitigates instances of recurring content and/or behaviors that suggest use of the service in a manner that may violate the Code of Conduct or other applicable product terms.

Azure OpenAI Service APIs and Keys

24. Microsoft provides access to the Azure OpenAI Service through application programing interfaces, also known as APIs. An API is computer code that enables software applications to communicate with each other. The Azure OpenAI Service APIs are divided into three categories. First, Microsoft's Azure control plane API is used for things like creating Azure OpenAI resources, model deployment, and other higher level resource management tasks. Azure OpenAI shares software and a common control plane with all other Azure AI Services. Second, Microsoft's data plane authoring API controls software that provides fine-tuning, file-upload, ingestion jobs, batch and certain model level queries. Third, Microsoft's data plane inference API accesses Microsoft software that provides the inference capabilities/endpoints for features like completions, chat completions, embeddings, speech/whisper, and DALL·E.[17]

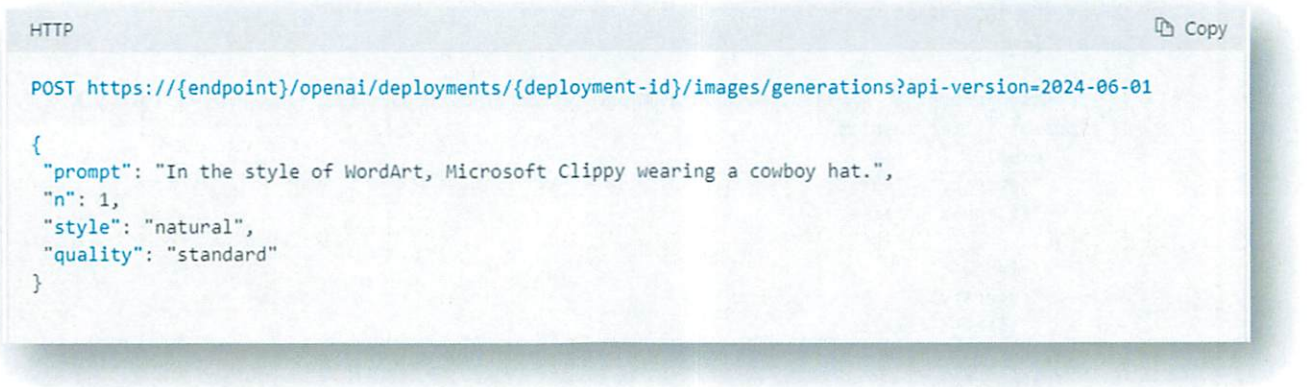
25. Customers who have entered into the necessary contractual agreements with Microsoft may use Microsoft's APIs to access the Azure OpenAI Service via the Internet using the http protocol. For instance, the example code in Figure 2 below depicts an API call to the Azure OpenAI Service that requests DALL·E to generate an image of Microsoft Clippy wearing a cowboy hat:

---

[16] https://learn.microsoft.com/en-us/azure/ai-services/openai/concepts/content-filter?tabs=warning%2Cuser-prompt%2Cpython-new; A true and correct copy of which is attached to the Index as Exhibit 22

[17] https://learn.microsoft.com/en-us/rest/api/azure/; A true and correct copy of which is attached to the Index as Exhibit 24

Fig. 2



26. The API-version field tells Microsoft's system which version of the API the customer is using. The "prompt" field is the text description of the desired image, "n" is the number of images requested, "style" refers to the image style requested, and quality refers to the image resolution (e.g., standard or high definition). Only by communicating in the specific format required by Microsoft's API can a customer access the functionality provided by the Azure OpenAI Service API.

27. In response to the API call in Figure 2 above, because there is no prohibited content or abuse detected, the Azure OpenAI Service returns the response depicted in Figure 3 below. The "revised_prompt" field indicates the prompt used by the Azure OpenAI Service to generate the image, and the "url" field is the uniform resource locator, e.g., the internet address, of the image generated by the Azure OpenAI Service.

Fig. 3

```
{
  "body": {
    "created": 1698342300,
    "data": [
      {
        "revised_prompt": "A vivid, natural representation of Microsoft Clippy wearing a cowboy hat.",
        "prompt_filter_results": {
          "sexual": {
            "severity": "safe",
            "filtered": false
          },
          "violence": {
            "severity": "safe",
            "filtered": false
          },
          "hate": {
            "severity": "safe",
            "filtered": false
          },
          "self_harm": {
            "severity": "safe",
            "filtered": false
          },
          "profanity": {
            "detected": false,
            "filtered": false
          }
        },
        "url": "https://dalletipusw2.blob.core.windows.net/private/images/e5451cc6-b1ad-4747-bd46-b89a3a3b8b
        "content_filter_results": {
          "sexual": {
            "severity": "safe",
            "filtered": false
          },
          "violence": {
            "severity": "safe",
            "filtered": false
          },
          "hate": {
            "severity": "safe",
            "filtered": false
          },
          "self_harm": {
            "severity": "safe",
            "filtered": false
```


28. In the example code above, there is no content filtering called for, so an image is successfully generated and returned to the URL specified in the url field. By contrast, when the Azure OpenAI Service content filtering system detects harmful content, a user receives either an

error on the API call if the prompt was deemed inappropriate, or the finish_reason on the response will be content_filter to signify that some of the completion was filtered.

29. In order to utilize Microsoft APIs to generate an image using DALL·E as described above, a user must authenticate themselves to gain access to the Azure OpenAI Service. The Azure OpenAI Service provides two methods for authentication: Microsoft Entra ID authentication or API Key authentication--For this type of authentication, all API requests must include the API Key in the api-key HTTP header.

30. An API key is a unique string composed of 52 randomly generated numbers and letters. API keys are used for data plane (content) requests and may be viewed and managed in the customer's Azure Portal. Key-based authentication is the default type of authentication for most Azure services. For this type of authentication, all API requests must include a valid API key in the api-key HTTP header.

31. By design, API keys are virtually impossible to re-create and provide a significant measure of security. However, like any lock-and-key system, API key security is only effective if the key itself is kept secure. For this reason, Microsoft advises its users to adhere to certain best practice regarding API key use and maintenance.

32. API keys can be accidentally exposed in public code repositories, for example, when keys are hardcoded into source code that is maintained in publicly accessible source code repositories. Bad actors have been known to create scraping tools designed specifically to search for API keys, and these tools can be applied in any code repository that the bad actor is able to access in order to steal API Keys for malicious purposes. Even when API Keys are maintained in secure environments, they are susceptible to theft by persons gaining unauthorized access to those environments, including during data breaches or the like. For this reason, Microsoft counsels against storing API Keys in unencrypted form.

Defendants' Unlawful Access to and Use Of the Azure OpenAI Service

33. In late July, 2024, Microsoft discovered use of customer API keys to generate prohibited content. Investigation revealed that the API keys had been stolen. The precise manner in which Defendants obtained all the API Keys used to carry out the misconduct described in this Complaint is unknown, but it appears that Defendants have engaged in a pattern of systematic API Key theft that enabled them to steal Microsoft Azure OpenAI Service API Keys from multiple Microsoft customers. Multiple customers from whom Defendants stole API keys are U.S. companies, including companies located in Pennsylvania and New Jersey.

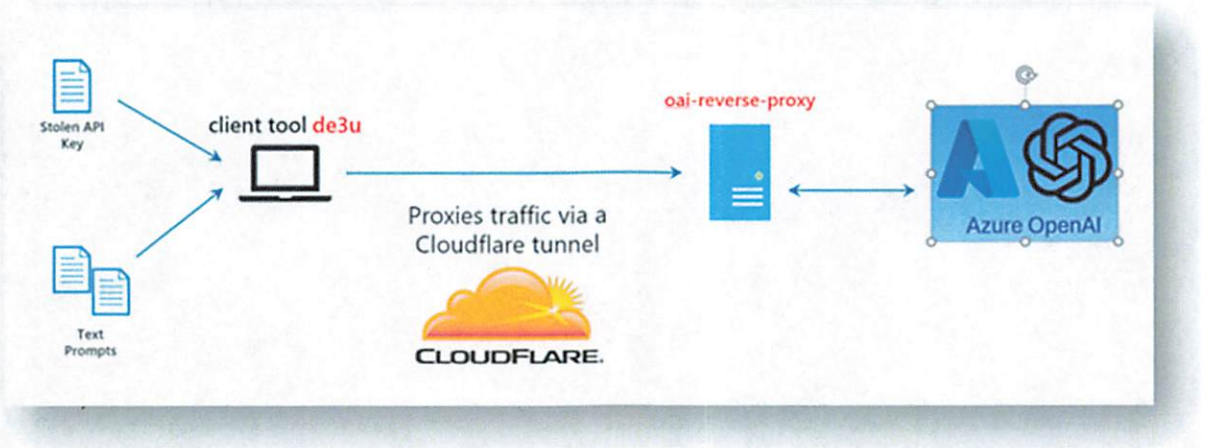
34. Using stolen Microsoft API keys that belonged to U.S.-based Microsoft customers, Defendants created a hacking-as-a-service scheme specifically designed to abuse Microsoft's Azure infrastructure and software. Defendants leveraged customized software and infrastructure to generate and communicate HTTP requests that included Azure OpenAI service API calls, stolen API keys, deployment ID, endpoint address and other information configured by the de3u software and oai reverse proxy.

35. Defendants sophisticated use of custom software and specially configured hardware allowed them to gain unauthorized access to and use of Microsoft computers running Azure OpenAI services software necessary for processing, routing, filtering, executing, and communicating responses to Azure OpenAI service API calls. Defendants could not have achieved the level of access they achieved without circumventing Microsoft's technological measures for limiting access to and use of the computers and software that comprise the Azure OpenAI service.

36. Defendants' malicious service can be described as two related software tools and associated Internet infrastructure used to unlawfully generate images through the Azure OpenAI Service. First, Defendants created client-side software tool referred to by Defendants as "de3u." Second, Defendants created software for running a reverse proxy service, referred to as the "oai reverse proxy", designed specifically for processing and routing communications from the de3u

software to Microsoft's systems. Figure 4 below depicts the basic architecture of Defendants malicious hacking-as-a-service infrastructure.

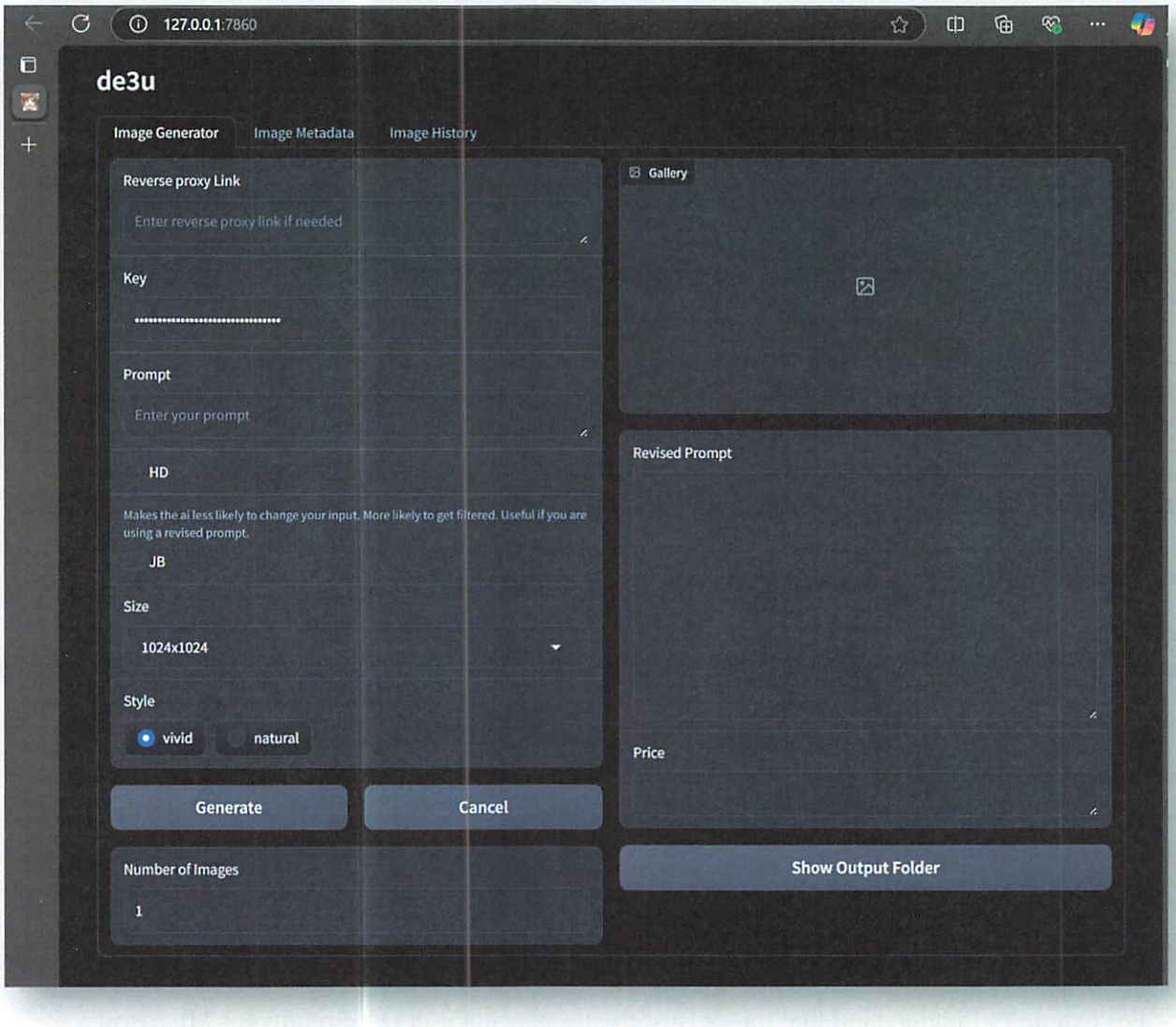
Fig. 4



37. **The de3u Software**. At a high level, the de3u software allows users to issue Microsoft API calls to generate images using the DALL-E model through a simple user interface that leverages the Azure APIs to access the Azure OpenAI Service. API calls through de3u are designed to be authenticated using stolen API keys and other authenticating information. I understand from communications with Microsoft investigator Rodel Finones and others that Microsoft's reverse engineering and investigative work show that the de3u software permits users to circumvent technological measures that control access to Azure computers and software. For example, I understand that the de3u software permits users to circumvent Microsoft measures that prevent alteration of certain Azure OpenAPI Service API request parameters, like endpoint associations.

38. I understand that Defendants' de3u software allows simple mapping of the control fields to input and output parameters so that less sophisticated bad actors can leverage stolen API keys without having to write their own code. Figure 5 below is a screen capture of the de3u user interface Defendants created:

Fig.5



39. Defendants designed their de3u software to be shared with third parties without the need for a hosting web server. In a web server configuration, users access software that is running on a computer connected to the internet.

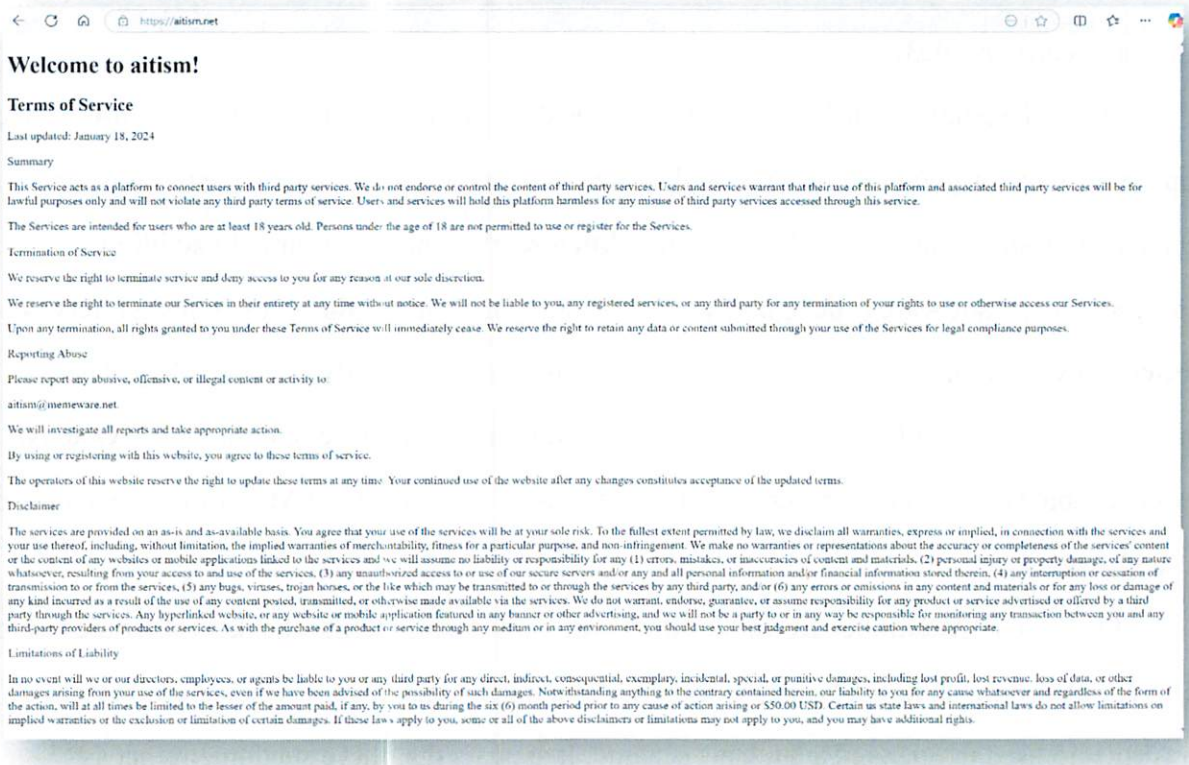
40. Defendants' system avoids the need for a web server, relying instead on a publicly accessible website at the URL "rentry.org/de3u." This allows Defendants to provide access to

their de3u tool—and by extension, access to the Azure OpenAI Service—to anyone in the world who visits rentry.org/de3u.

41. Defendants' de3u software is designed to try to prevent the Azure OpenAI service from revising the original text prompt used to generate images, which can happen, for example, when a text prompt contains words that trigger Microsoft's content filtering. In addition, Defendants' de3u software is designed to detect and report whether the Azure OpenAI Service rejected a text prompt because it is considered violative of Microsoft's content policy. These features, combined with Defendants' unlawful programmatic API access to the Azure OpenAI service, enabled de3u users to reverse engineer means of circumventing Microsoft's content and abuse measures.

42. **The Aitism.net Domain.** Microsoft's investigation into the de3u software led to discovery of several subdomains of the website "aitism.net" that appear to be part of the static infrastructure used to operate Defendants scheme. It appears that these subdomains act as pointers for the de3u software and oai reverse proxy service discussed below. Users can cut and paste URLs for aitism.com subdomains into the de3u software to tell the de3u software and oai reverse proxy service which company's generative AI services they want to abuse. A true and correct copy of the WHOIS record for the aitism.net domain is attached to the Index of Evidence as Exhibit 4.

43. The top-level website on the "aitism.com" domain provides terms of use for the service Defendants are providing. A true and correct screen shot of the website accessible on the aitism.com domain is depicted below and attached to the Index as Exhibit 5.



https://aitism.net

Welcome to aitism!

Terms of Service

Last updated: January 18, 2024

Summary

This Service acts as a platform to connect users with third party services. We do not endorse or control the content of third party services. Users and services warrant that their use of this platform and associated third party services will be for lawful purposes only and will not violate any third party terms of service. Users and services will hold this platform harmless for any misuse of third party services accessed through this service.

The Services are intended for users who are at least 18 years old. Persons under the age of 18 are not permitted to use or register for the Services.

Termination of Service

We reserve the right to terminate service and deny access to you for any reason at our sole discretion.

We reserve the right to terminate our Services in their entirety at any time without notice. We will not be liable to you, any registered services, or any third party for any termination of your rights to use or otherwise access our Services.

Upon any termination, all rights granted to you under these Terms of Service will immediately cease. We reserve the right to retain any data or content submitted through your use of the Services for legal compliance purposes.

Reporting Abuse

Please report any abusive, offensive, or illegal content or activity to:

aitism@memeware.net

We will investigate all reports and take appropriate action.

By using or registering with this website, you agree to these terms of service.

The operators of this website reserve the right to update these terms at any time. Your continued use of the website after any changes constitutes acceptance of the updated terms.

Disclaimer

The services are provided on an as-is and as-available basis. You agree that your use of the services will be at your sole risk. To the fullest extent permitted by law, we disclaim all warranties, express or implied, in connection with the services and your use thereof, including, without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. We make no warranties or representations about the accuracy or completeness of the services' content or the content of any websites or mobile applications linked to the services and we will assume no liability or responsibility for any (1) errors, mistakes, or inaccuracies of content and materials, (2) personal injury or property damage, of any nature whatsoever, resulting from your access to and use of the services, (3) any unauthorized access to or use of our secure servers and/or any and all personal information and/or financial information stored therein, (4) any interruption or cessation of transmission to or from the services, (5) any bugs, viruses, trojan horses, or the like which may be transmitted to or through the services by any third party, and/or (6) any errors or omissions in any content and materials or for any loss or damage of any kind incurred as a result of the use of any content posted, transmitted, or otherwise made available via the services. We do not warrant, endorse, guarantee, or assume responsibility for any product or service advertised or offered by a third party through the services. Any hyperlinked website, or any website or mobile application featured in any banner or other advertising, and we will not be a party to or in any way be responsible for monitoring any transaction between you and any third-party providers of products or services. As with the purchase of a product or service through any medium or in any environment, you should use your best judgment and exercise caution where appropriate.

Limitations of Liability

In no event will we or our directors, employees, or agents be liable to you or any third party for any direct, indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profit, lost revenue, loss of data, or other damages arising from your use of the services, even if we have been advised of the possibility of such damages. Notwithstanding anything to the contrary contained herein, our liability to you for any cause whatsoever and regardless of the form of the action, will at all times be limited to the lesser of the amount paid, if any, by you to us during the six (6) month period prior to any cause of action arising or $50.00 USD. Certain us state laws and international laws do not allow limitations on implied warranties or the exclusion or limitation of certain damages. If these laws apply to you, some or all of the above disclaimers or limitations may not apply to you, and you may have additional rights.

44. A true and correct screen shot of the website (rentry.org/miniproxy) where Defendants advertise the aitism.com subdomains pointers for the reverse proxy service is depicted below and attached to the Index as Exhibit 6.

MINIPROXY <3

proxy links

~~https://leone-harvest-suppliers-tcp.trycloudflare.com (azure and api dall-e can be used for token lookups and nickname changes. open to everyone)~~
https://assistant.aitism.net/assistant/miniproxy/openai (gpt-4, gpt-4-turbo, gpt-4o, gpt-3.5-turbo, o1)
https://assistant.aitism.net/assistant/miniproxy/azure (32k, 4o)
https://assistant.aitism.net/assistant/miniproxy/aws (aws claude)
https://assistant.aitism.net/assistant/miniproxy/anthropic (claude api)
https://assistant.aitism.net/assistant/miniproxy/gemini (gemini. new exp model available)
https://assistant.aitism.net/assistant/miniproxy/gcp (experimental. no opus)
enable streaming if you receive timeout errors. Cloudflare has a 100 second limit. ignore the model list the proxy sends you.

```
openai context size: 131072
anthropic context size: 25000
openai output size: 16384
anthropic output size: 4000
"allowAwsLogging": "false",
"promptLogging": "false",
```

new usage graphs soon

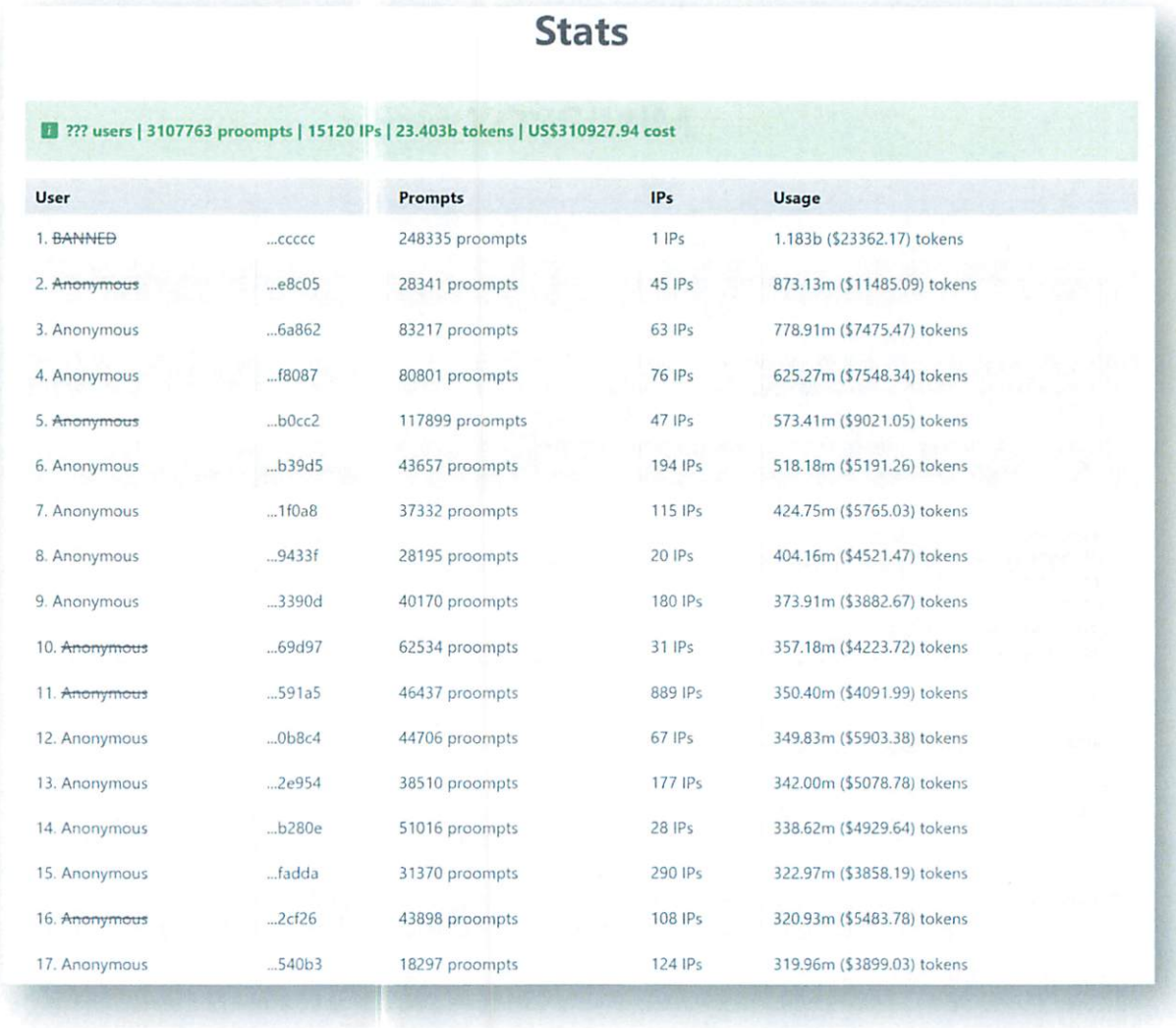
total **active** users: 145 (CLOSED)

if any model is broken/dead pls lmk with an email and i will try to fix. i cant always check because uni and stuff... im not leaving for a while you don't need to worry

news (now)

added o1 (non preview!)
checking emails tmr i have like 20

45. Defendants also publish on the rentry.org/miniproxy website user statistics and the costs (in tokens) associated with use of Defendants services. A true and correct screen shot of this data is depicted below and attached to the Index as Exhibit 7.



Stats

??? users | 3107763 proompts | 15120 IPs | 23.403b tokens | US$310927.94 cost

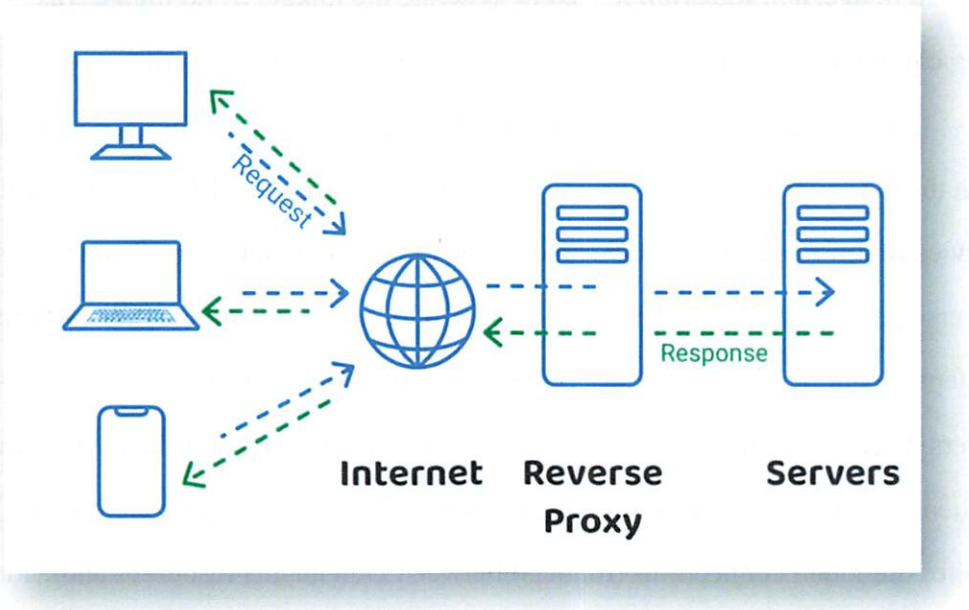
User		Prompts	IPs	Usage
1. ~~BANNED~~	...ccccc	248335 proompts	1 IPs	1.183b ($23362.17) tokens
2. ~~Anonymous~~	...e8c05	28341 proompts	45 IPs	873.13m ($11485.09) tokens
3. Anonymous	...6a862	83217 proompts	63 IPs	778.91m ($7475.47) tokens
4. Anonymous	...f8087	80801 proompts	76 IPs	625.27m ($7548.34) tokens
5. ~~Anonymous~~	...b0cc2	117899 proompts	47 IPs	573.41m ($9021.05) tokens
6. Anonymous	...b39d5	43657 proompts	194 IPs	518.18m ($5191.26) tokens
7. Anonymous	...1f0a8	37332 proompts	115 IPs	424.75m ($5765.03) tokens
8. Anonymous	...9433f	28195 proompts	20 IPs	404.16m ($4521.47) tokens
9. Anonymous	...3390d	40170 proompts	180 IPs	373.91m ($3882.67) tokens
10. ~~Anonymous~~	...69d97	62534 proompts	31 IPs	357.18m ($4223.72) tokens
11. ~~Anonymous~~	...591a5	46437 proompts	889 IPs	350.40m ($4091.99) tokens
12. Anonymous	...0b8c4	44706 proompts	67 IPs	349.83m ($5903.38) tokens
13. Anonymous	...2e954	38510 proompts	177 IPs	342.00m ($5078.78) tokens
14. Anonymous	...b280e	51016 proompts	28 IPs	338.62m ($4929.64) tokens
15. Anonymous	...fadda	31370 proompts	290 IPs	322.97m ($3858.19) tokens
16. ~~Anonymous~~	...2cf26	43898 proompts	108 IPs	320.93m ($5483.78) tokens
17. Anonymous	...540b3	18297 proompts	124 IPs	319.96m ($3899.03) tokens

46. Gaining control over the aitism.com domain would be an important step in remediating and investigating Defendants conduct for two primary reasons. First, gaining control over the aitism.com domain would permit Microsoft to "sinkhole" the domain so that the subdomains can no longer serve as pointers for attacks on generative AI services. Second, gaining control over the aitism.com domain may result in collection of attribution evidence and other information related to use of the domain. For example, in the past, Microsoft's control over malicious domains has yielded evidence about operators of that domain or the substance of communications (e.g., API calls) sent to the domain.

47. **The "oai" Reverse Proxy Service**. Defendants have implemented and used an "oia" reverse proxy service through which de3u users can access the Azure OpenAI Service. Defendant's oai reverse proxy service consists of software running on a reverse proxy server that acts as a tunnel from de3u user computers into the Azure OpenAI Service.

48. In general, a reverse proxy server is a server that sits in front of web servers and forwards client (e.g. web browser) requests to those web servers. A reverse proxy ensures that no client ever communicates directly with that origin server, as depicted in Figure 5 below.

Fig. 5



49. In addition to performing the traditional function of any reverse proxy (e.g., forwarding requests), Defendants oai reverse proxy tool processes and alters communications traffic between de3u client computers and the target Azure OpenAI service. Defendants specifically configured the oai reverse proxy to route traffic to a list of Azure OpenAI Service endpoints and corresponding stolen credentials. When a de3u user sends a request to the Azure OpenAI service to generate an image, the de3u software routes the request to the oai reverse

proxy tunnel address. The oai reverse proxy tool parses the request and, for attacks on Azure, reconfigures the API call with a stolen Azure API Key and associated authentication information before forwarding the call to the Azure OpenAI service target endpoint via a Cloudflare tunnel. The request forwarded by the oai reverse proxy tunnel includes stolen API keys and associated endpoints (authentication information).

50. The oai reverse proxy tool also receives and processes responses from the Azure OpenAI service before forwarding responses and other data to the de3u user device. If the de3u user's prompt resulted in generation of an image by the Azure OpenAI service, then the oai reverse proxy tool receives image parameters from the Azure OpenAI service including the URL of the generated image, and the prompt used to generate the image. If no image was generated, the oai reverse proxy tool receives and logs the results of any content filtering.

51. If the de3u user's prompt resulted in generation of an image by the Azure OpenAI service, then the oai reverse proxy tool retrieves the image from the URL specified in the Azure OpenAI service return response and saves the image to the computer at an IP address associated with the reverse proxy service ("AWS IP Address"). The oai proxy service then performs several additional steps including injecting proxy information into the response traffic, setting some HTTP headers, logging events and text prompts, and sending the traffic back to the requesting de3u user client computer. These communications are all routed through a CloudFlare Tunnel that establishes outbound connections (tunnels) between Defendants resources and Cloudflare's global network. A Cloudflare Tunnel is a persistent object that routes traffic to DNS records.[18]

Defendants' Conduct Related to the Eastern District of Virginia and United States

52. I am informed and believe based on Microsoft's investigation to date that Defendant DOE 1 is a natural person with access to and control over at least the website located at rentry.org/de3u, the source code repositories located at "github.com/notfiz/de3u," and stolen Azure API keys and other authentication information. DOE 1 appears to resided outside the United States.

---

[18] https://developers.cloudflare.com/cloudflare-one/connections/connect-networks/; Exhibit 25

53. DOE 1 chose a ".org" domain, "rentry.org/de3u" as the access point for the tools used to carry out Azure Abuse Enterprise. Since 1984, the ".org" top level domain ("TLD") has been managed by the Public Interest Registry ("PIR"), based in Reston, Virginia. This means that whenever Defendants or third parties access Defendants' tools through Defendants' "rentry.org/de3u" website ("Gateway Domain"), that access depends on PIR's physical domain name servers ("DNS") and DNS routing services. As a sophisticated actor who has demonstrated substantial knowledge of computer networks and the Internet, I would expect DOE 1 to know and understand that by selecting a ".org" TLD for the Gateway Domain website, Defendants would be relying on hardware and services provided by PIR from Reston, Virginia, to effect their scheme. I would certainly expect DOE 1 to understand that use of a ".org" domain depends on use of U.S.-based computers where the .org TLD administrator resides.

54. I am informed and believe based on Microsoft's investigation to date that Defendant DOE 3 is a natural person with access to and control over instrumentalities used in connection with the violations of law described in the Complaint, including reverse proxy tool infrastructure, the domain "atism.net," and the AWS IP Address used to carry out the Azure Abuse Enterprise. This domain provides instructions on how to use Defendants malicious infrastructure and also appears to be associated with the network architecture used by Defendants to abuse AI services provided by Microsoft and others. I am informed and believe that obtaining control over the atism.net domain will undermine Defendants ability to operate their Azure Abuse Enterprise infrastructure and is likely to yield valuable evidence about Defendants conduct and use of the atism.net domain that may otherwise be lost, especially if Defendants receive prior notice of Microsoft's intent to secure such evidence.

55. DOE 3 chose a ".net" domain for supporting its reverse proxy service. Since 2000, the ".net" TLD has been managed by Verisign, Inc., based in Reston, Virginia. This means that whenever Defendants or third parties access Defendants' tools via the atism.net domain, that access depends on Verisign's physical DNS and DNS routing services. As a sophisticated actor who has demonstrated substantial knowledge of computer networks and the Internet, I would

expect DOE 3 to know and understand that by selecting a ".net" TLD for the Gateway Domain website, Defendants would be relying on hardware and services provided by Verisign from Reston, Virginia, to effect their scheme. I would certainly expect DOE 3 to understand that use of a ".net" domain depends on use of U.S.-based computers where the .net TLD administrator resides.

56. In addition, DOE 3 chose the AWS IP Address as one end of the access tunnel they created into the Azure OpenAI Service in order to carry out their scheme. The AWS IP Address geolocates to computers physical located in Virginia. Defendants, sophisticated actors who have demonstrated substantial knowledge of computer networks, almost certainly know the geolocation of the AWS IP Address, which is easily ascertainable from by Internet user who knows the AWS IP address.

57. In addition to relying on infrastructure located within the Eastern District of Virginia, the Azure Abuse Enterprise also used services, technology, and infrastructure located in other parts of the United States. For example, Defendants intentionally:

- configured their software and systems to use physical machines, technology, and services provided in and from the United States by Microsoft (including, for example, Microsoft Azure servers, technology, and services);
- configured their software and systems to use physical machines, technology, and services provided in and from the United States by Amazon Web Services ("AWS"), a U.S. company;
- configured their software and systems to use physical machines, technology, and services provided in and from the United States by Cloudflare, a U.S. company;
- configured their software and systems to use physical machines, technology, and services provided in and from the United States by PIR,
- configured their software and systems to use physical machines, technology, and services provided in and from the United States by Verisign,
- configured their software and systems to victimize Microsoft, OpenAI, AWS, Cloudflare,

PIR, and Verisign

- configured their software and systems to create and distribute harmful images within the U.S

Efficacy of the Requested Relief

58. Microsoft acted promptly to investigate and remediate Defendants' conduct. Although Microsoft has largely remediated the technical exploits Defendants initially leveraged to carry out the Azure Abuse Enterprise, Defendants continue to control stolen API keys, internet infrastructure, and malicious software tools that can be deployed to carry out the illegal conduct described herein.

59. Based on my experience dealing with sophisticated cybercriminals like Defendants, it is my belief that maintaining this action under seal for a brief period is important to ensuring that any orders issued by the Court can be carried out before Defendants have an opportunity to move their infrastructure and/or destroy potential evidence. For example, if given notice of this action or Microsoft's request for a temporary restraining order, Defendants would be able to redirect traffic that is currently directed to the aitism.com domains and could also delete evidence that third party ISPs would otherwise preserve in response to Microsoft's subpoenas.

60. Based on my experience dealing with sophisticated cybercriminals like Defendants, I believe it will be difficult to quickly identify physical address information for Defendants. I also believe that the best way to provide Defendants with actual notice and service of process in this case is through the email accounts associated with Defendants that Microsoft has uncovered during its investigation, as well as through any third-party ISP abuse contact channels associated with Defendants infrastructure. Microsoft has not seen any evidence to indicate that any Defendant resides in a jurisdiction that is subject to the Hague Convention on International Service.

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct to the best of my knowledge, information, and belief. Executed this 19th day of December 2024 at Alexandria, Virginia.

Jason Lyons